(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 198 11 720 A 1**

(51) Int. Cl.[6]: H 04 L 9/32

(21) Aktenzeichen: 198 11 720.5
(22) Anmeldetag: 18. 3. 98
(43) Offenlegungstag: 30. 9. 99

DE 198 11 720 A 1

(71) Anmelder:
Kobil Computer GmbH, 67547 Worms, DE

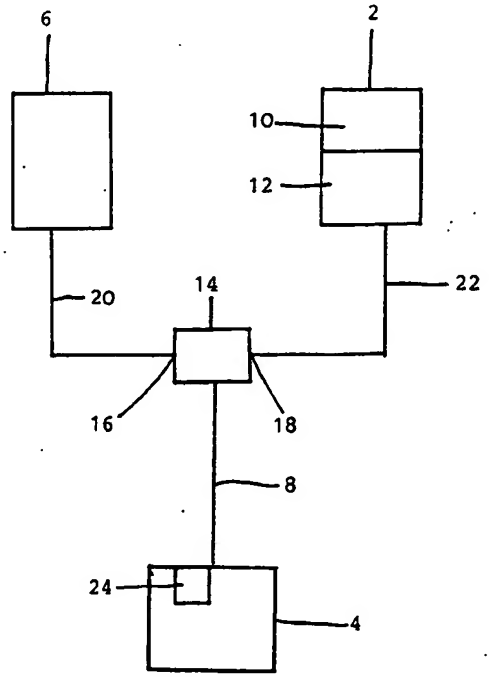
(72) Erfinder:
Koyun, Ismet, 67547 Worms, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Vorrichtung zum Erstellen einer digitalen Signatur

(57) Eine Vorrichtung zum Erstellen einer digitalen Signatur enthält einen Computer (4) und ein externes Ausgabegerät (6). Die Vorrichtung soll dahingehend weitergebildet werden, daß ein Benutzer sicher sein kann, nur das von ihm gewünschte Dokument zu signieren und nichts anderes. Es wird vorgeschlagen, zwischen dem Computer (4), insbesondere dessen Zentraleinheit, und dem externen Ausgabegerät (6) ein sicheres Modul (2) zur Berechnung der digitalen Signatur mit Hilfe eines Secret Key anzuordnen.



DE 198 11 720 A 1

Beschreibung

Die Erfindung bezieht sich auf eine Vorrichtung zum Erstellen einer digitalen Signatur gemäß den im Oberbegriff des Patentanspruchs 1 angegebenen Merkmalen.

In zunehmendem Maße möchten EDV-Anwender heute elektronische Dokumente über unsichere Netze (Telefonnetz, Internet) versenden. Es stellt aus technischer Sicht kein Problem dar, ein im Klartext vorliegendes (d. h. insbesondere unverschlüsseltes) elektronisches Dokument auf seinem Weg vom Absender zum Empfänger zu verfälschen oder gar den Absender zu fälschen. Dennoch soll der Empfänger absolut verläßlich prüfen können, ob ein erhaltenes elektronisches Dokument tatsächlich vom angegebenen Absender stammt und auf dem Weg zum Empfänger nicht verändert wurde. Darüber hinaus möchte der Empfänger im Streitfalle Dritten gegenüber beweisen können, daß er ein bestimmtes Dokument von einer bestimmten Person/Institution erhalten hat. Dies erfordert sozusagen ein elektronisches Analogon zu der konventionellen handschriftlichen Unterschrift. Die Kryptographie bietet hier eine Lösung: sogenannte digitale Signaturverfahren. Mittels digitaler Signatur soll dem Empfänger eines Dokuments ein rechtsverbindlicher Beweis dafür geliefert werden, daß das Dokument auch tatsächlich vom ausgewiesenen Sender stammt und auf dem Übertragungswege nicht verfälscht wurde. Umgekehrt hat der Sender ein Interesse an einem solchen Beweis dahingehend, daß der richtige Empfänger das Dokument auch unverfälscht erhalten hat. Zur Gewährleistung der Sicherheit, d. h. der Unverfälschbarkeit einer digitalen Signatur müssen insbesondere folgende Bedingungen erfüllt sein:

1. Der Secret Key des Benutzers, der die mathematische Funktion zum Signieren eines elektronischen Dokumentes parametrisiert, muß absolut geheim bleiben.
2. Der Algorithmus zum Signieren eines Dokumentes darf nicht manipulierbar sein. Er wird in einer sicheren physikalischen Umgebung (z. B. durch eine Chipkarte) ausgeführt.
3. Der Benutzer muß sich sicher sein, daß er genau das von ihm gewünschte Dokument signiert und nichts anderes.

Wegen der Bedingungen 1 und 2 stimmen Experten darin überein, daß der Secret Key des Benutzers im von außen nicht zugänglichen Bereich einer Chipkarte gespeichert werden sollte, welche über die Fähigkeit verfügt, mit Hilfe dieses Keys die digitale Signatur zu einem vorgegebenen Dokument zu berechnen. Ein Lösungsvorschlag, der zudem noch Bedingung 3 erfüllt, ist derzeit noch nicht bekanntgeworden.

Das typische derzeit für die Praxis favorisierte System zum Signieren elektronischer Dokumente zeigt ein Dokument auf einem Monitor oder Display an, worauf der Benutzer (menügesteuert) den Befehl gibt, dieses Dokument durch seine Chipkarte signieren zu lassen. Ob dann tatsächlich das zuvor angezeigte Dokument signiert wird, ist allerdings nicht gewährleistet, denn der benutzte Computer könnte so manipuliert sein, daß der an den Computer angeschlossene Chipkartenleser zum Signieren ein Dokument erhält, welches sich von dem zuvor am Monitor oder Display angezeigten – vielleicht nur geringfügig – unterscheidet.

Hiervon ausgehend liegt der Erfindung die Aufgabe zugrunde, die Vorrichtung der genannten Art dahingehend weiterzubilden, daß der Benutzer sicher sein kann, daß er genau das von ihm gewünschte Dokument signiert und nichts anderes. Die Vorrichtung soll mit geringem Aufwand das bislang ungelöste Teilproblem, welches auch als Darstellungsproblem bezeichnet wird, beim fälschungssicheren Signieren elektronischer Dokumente mit einem geringen Aufwand lösen. Ferner soll die Vorrichtung für den Anwender in einfacher Weise durchschaubar sein und eine einfache Anordnung der zum Einsatz gelangenden peripheren Hardwarekomponenten ermöglichen.

Die Lösung dieser Aufgabe erfolgt gemäß den im Patentanspruch 1 angegebenen Merkmalen.

Die vorgeschlagene Vorrichtung zeichnet sich durch einen einfachen und funktionsgerechten Aufbau aus und löst in zweckmäßiger Weise das Darstellungsproblem bei der Erzeugung digitaler Signaturen. Durch die Durchschaubarkeit der einfachen Steueranordnung und der verwendeten peripheren Hardwarekomponenten ist es für den Computeranwender ohne weiteres ersichtlich, daß das sichere signierende Modul, wie insbesondere die Chipkarte und das Chipkartenterminal, genau die gleichen Daten oder Signale als Eingabe erhält wie das genannte externe Ausgabegerät. Das sichere Modul, welches den zum Signieren notwendigen Secret Key dauerhaft speichert und welches mit Hilfe dieses Secret Keys die digitale Signatur eines vorgegebenen elektronischen Dokuments oder einer vorgegebenen Datei berechnet und diesem definiert zuordnet, wird in zweckmäßiger Weise zwischen den Computer, und zwar insbesondere dessen Zentraleinheit, und das externe Ausgabegerät geschaltet. Darüber hinaus ist das zwischengeschaltete sichere Modul derart ausgebildet, daß erfindungsgemäß die Korrektheit einer vorgegebenen digitalen Signatur für ein vorgegebenes elektronisches Dokument überprüfbar ist. Das Ausgabegerät kann als Monitor bzw. Display oder als Drucker bzw. Plotter ausgebildet sein. Das sichere Modul und das Ausgabegerät sind über bevorzugt frei verlegte sichtbare Datenkabel und eine Kopplungskomponente derart miteinander verbunden, daß das sichere Modul und das externe Ausgabegerät stets die gleichen Daten empfangen. Die Kopplungskomponente, welche in zweckmäßiger Weise als ein T-Stück zur Verbindung der Datenkabel ausgebildet sein kann, besitzt keine weiteren Fähigkeiten, als das Weiterleiten der vom Computer erhaltenen Daten an die beiden Ausgänge, die auf das sichere Modul und ferner auf das externe Ausgabegerät geführt sind.

In einer besonderen Weiterbildung der Erfindung ist ein Druckertreiber für Postscriptdrucker derart vorgesehen, daß mit der Ausgabe eines Druckbefehls, insbesondere einer Postscriptdatei, in dem sicheren Modul die Durchführung der Signatur der zugeordneten Datei erfolgt, welche vom Drucker ausgegeben wird.

Besondere Ausgestaltungen und Weiterbildungen der Erfindung sind in den Unteransprüchen sowie der weiteren Beschreibung eines besonderen Ausführungsbeispiels angegeben.

Fig. 1 zeigt schematisch ein Blockschaltbild der Vorrichtung mit einem sicheren Modul **2**, welches den zum Signieren eines Dokuments notwendigen Secret Key dauerhaft speichert. Das sichere Modul ermöglicht ferner mittels des genannten Secret Keys die digitale Signatur für ein elektronisches Dokument oder eine vorgegebene Datei. Das genannte Dokument bzw. die Datei wird mittels eines Computers **4**, insbesondere dessen Zentraleinheit, bereitgestellt und zu einem externen Ausgabegerät über eine bevorzugt frei verlegte und/oder sichtbare Datenleitung **8** geleitet. Das Ausgabegerät **6** dient zur Ausgabe der Daten in sichtbarer Form und ist als Monitor bzw. Display oder Drucker bzw. Plotter ausgebildet. Das sichere Modul **2** ist zwischen dem Computer **4** und dem Ausgabegerät **6** installiert und enthält parallel zu diesem exakt die gleichen Daten oder Dateien wie das externe Ausgabegerät **6**. In zweckmäßiger Weise ist die Datenleitung **8** für einen Benutzer sichtbar als Kabel ver-

legt, und zwar vorzugsweise als konventionelles Druckerkabel oder Monitorkabel. Für den Anwender ist somit unmittelbar aufgrund der einfachen Verbindung der externen Komponenten erkennbar, daß in das externe Ausgabegerät die gleichen Daten gelangen wie in das sichere Modul, welches zwischen der Zentraleinheit des Computers und dem externen Ausgabegerät **6** installiert ist. Das zwischengeschaltete sichere Modul **2** ist in besonders zweckmäßiger Weise zur Überprüfung einer vorgegebenen digitalen Signatur für ein vorgegebenes elektronisches Dokument ausgebildet.

In bevorzugter Weise enthält das sichere signierende Modul **2** einerseits eine Prozessorchipkarte, in welcher insbesondere der Secret Key gespeichert ist, und andererseits ein Chipkartenterminal **12** zum Ansteuern der Chipkarte **10**. Das Modul **2** ermöglicht erfindungsgemäß ferner, in der beschriebenen Anordnung die Korrektheit einer vorgegebenen digitalen Signatur für ein vorgegebenes elektronisches Dokument zu überprüfen.

In besonders zweckmäßiger Weise erfolgt die Verbindung des Computers **4** bzw. dessen zentralen Einheit mit dem sicheren Modul **2** sowie dem externen Ausgabegerät **6** über eine Kopplungskomponente **14**. Es handelt sich hierbei um eine passive Kopplungskomponente, vorzugsweise in Form eines T-Stücks, welches einerseits an die mit dem Computer **2** verbundenen Datenleitung **8** angeschlossen ist und dessen Ausgänge **16**, **18** andererseits über Datenleitungen **20**, **22** mit dem externen Ausgabegerät **6** bzw. dem Modul **2** verbunden sind. Die Kopplungskomponente **14** besitzt keine weiteren Fähigkeiten als das Weiterleiten der vom Computer **4** eingehenden Daten an die beiden Ausgänge **16**, **18** und über die Kabel **20**, **22** zum externen Ausgabegerät **6** sowie zum Modul **2** bzw. Chipkartenterminal **12**. Für einen Anwender ist somit aufgrund der Einfachheit der Kopplungskomponente, welche keine weitere oder andere Funktionalität als das Weiterleiten der vom Computer **4** erhaltenen Daten an das Ausgabegerät **6** sowie an das das sichere Modul **2** aufweist, unmittelbar erkennbar, daß die gleichen Daten des Computers **4** sowohl an das Modul **2** als auch an das Ausgabegerät **6** gelangen.

In einer besonderen Weiterbildung ist dem Computer **4** ein Druckertreiber **24** zugeordnet, welcher einen üblichen Druckertreiber ersetzt. Der erfindungsgemäße Druckertreiber **24** ist derart ausgebildet, daß mit Ausgabe eines Druckbefehls, insbesondere für eine Postscript-Datei, in dem sicheren Modul **2** die Durchführung der Signatur der nachfolgenden Datei initiiert wird, welche auf dem externen Ausgabegerät bzw. Drucker **6** über den Ausgang **16** und die Datenleitung **20** ausgegeben wird.

Bezugszeichenliste

2 sicheres Modul
4 Computer
6 Ausgabegerät
8 Datenleitung
10 Prozessorchipkarte
12 Chipkartenterminal
14 Kopplungskomponente
16, **18** Ausgang
20, **22** Datenleitung/Kabel
24 Druckertreiber

Patentansprüche

1. Vorrichtung zum Erstellen einer digitalen Signatur, enthaltend einen Computer (**4**) und ein externes Ausgabegerät (**6**), **dadurch gekennzeichnet**, daß zwischen dem Computer (**4**), insbesondere dessen Zentraleinheit, und dem externen Ausgabegerät (**6**) ein sicheres Modul (**2**) angeordnet ist, zur Berechnung der digitalen Signatur mit Hilfe eines Secret Key.

2. Vorrichtung nach Anspruch 1, dadurch gekennzeichnet, daß das sichere Modul (**2**) ein Chipkartenterminal (**12**) sowie eine Prozessorchipkarte (**10**) zum dauerhaften Speichern des Secret Key enthält.

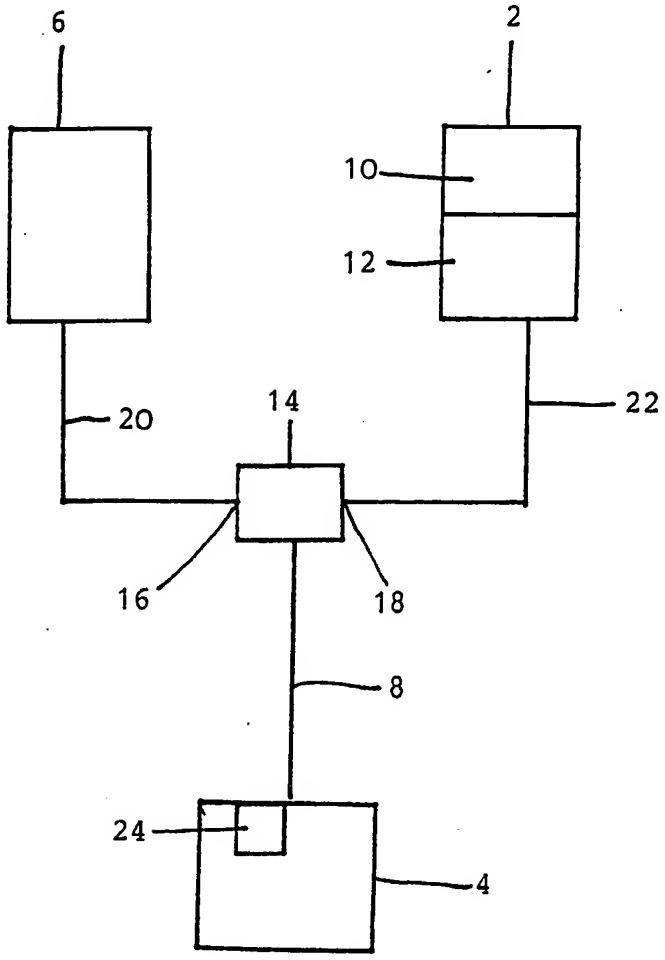
3. Vorrichtung nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß mit dem Computer (**4**) eine Kopplungskomponente (**14**) verbunden ist, deren Ausgänge (**16**, **18**) zum einen auf das externe Ausgabegerät (**6**) und zum anderen auf das sichere Modul (**2**), insbesondere über Datenleitungen oder Kabel (**20**, **22**) geführt sind.

4. Vorrichtung nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß bevorzugt über die Kopplungskomponente (**14**) das Ausgabegerät (**6**) und das sichere Modul (**2**) derart miteinander verbunden sind, daß das Ausgabegerät (**6**) und das sichere Modul (**2**) immer die gleichen Daten vom Computer (**4**) empfangen.

5. Vorrichtung nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß der Computer (**4**) einen derart ausgebildeten Druckertreiber enthält, daß mit der Ausgabe eines Druckbefehls im sicheren Modul (**2**) insbesondere im Chipkartenterminal (**12**) die Durchführung der Signatur der vom Computer (**4**) mit dem Druckbefehl ausgegebenen Datei initiiert wird.

Hierzu 1 Seite(n) Zeichnungen

Nummer: DE 198 11 720 A1
Int. Cl.[6]: H 04 L 9/32
Offenlegungstag: 30. September 1999



The invention relates to a device for producing a digital signature according to the characteristics set forth in the preamble of claim 1.

Increasingly more so, users of electronic data processing systems would nowadays like to send electronic documents by insecure networks (telephone, Internet). From a technical standpoint there is no difficulty in forging an existing document in readable text (that is, particularly un-encoded) in its path between the emitter and receiver, or even in falsifying the receiver. Moreover, the receiver should be able to confirm in a fully reliable manner that an electronic document received in fact originates from the referred emitter and that it has not been altered in its path to the receiver. For this reason, in case of a disagreement the receiver would like to be able to prove to a third party that a certain document was received from a given person or institution. This requires, so to speak, an electronic symbol in respect of the traditional manual signature. Cryptography provides a solution at this point: so-called digital signature procedures. By means of a digital signature the receiver of a document must be provided with a legally valid proof that the document was in fact sent by the referred emitter and that it was not falsified in the transmission path. Inversely, the emitter is also interested in that by a proof of this sort the correct receiver receives the document un-falsified. To ensure security, that is, the impossibility of forging a digital signature, the following conditions must be met:

1. The secret code of the user, that parameterizes the mathematical function to sign an electronic document, must remain absolutely secret.

2. The algorithm used to sign a document cannot be manipulated. This shall take place in a physically secure environment (such as in a chip card).

3. The user must be sure that he/she has signed the document presented to him/her, and not another one.

Because of conditions 1 and 2, experts agree that the user's secret code should be memorized in a zone of the chip card that is not accessible from the outside, which chip card can with the aid of said code calculate the digital signature for a predetermined document. To this date no solution has been proposed that also meets condition 3.

The system favored in practice for signing electronic documents displays a document on a monitor or screen on which the user (via a menu) instructs that a document be signed with the chip card. Whether in fact it is the document

that is displayed that is being signed is not truly ensured, as the computer employed may be manipulated so that the chip card reader connected to the computer receives a document for signature other than the one shown previously, maybe only for a brief time, on the monitor or screen.

In view of this, the invention is meant to develop in depth a device of the type described above so that the user may be certain that the desired document is signed, and not another. The device must solve with a low cost the partial problem not hitherto solved, which can also be identified as a display problem of the un-falsifiable signature for electronic documents. In addition, the invention must be visible in a simple manner for the user and must allow a simple connection of the peripheral hardware components used.

The solution to this mission is obtained by the characteristics shown in claim 1.

The device taught stands out for its simple construction in accordance with its function, and adequately solves the problem of display during the generation of a digital signature. Given the possibility of observing the simple control arrangement and the peripheral hardware components the user can easily appreciate that the safe signature module, and especially the chip card and the chip card terminal, receive exactly the same input data or signals as the aforementioned external output device. The secure module, that stores permanently the secret code required for the signature and with the aid of said secret code calculates the electronic signature of a predetermined electronic document or file and relates them in a defined manner with said code, is suitably connected to the computer, and more specifically between the central unit of the computer and the external output device. Because of the above the secure module interposed is designed such that in accordance with the invention it is possible to check whether a predetermined digital signature is correct for a predetermined electronic document. The output device may consist of a monitor or a screen, or a printer or plotter. The secure module and the output device are connected to each other preferably by visible, unobstructed data cables and with a coupling component such that the secure module and the external output module always receive the same data. The coupling components, which in a suitable form may be built as a T-connector to join the data cable, has no other capability than to transmit the data received from the computer to the two outputs, which lead to the secure module and the

external output device.

In a special development of the invention a printer control is provided for postscript printing, so that by issuing a printing instruction, particularly of a postscript file, the associated files are signed by the secure module, which is indicated by the printer.

Special configurations and developments of the invention are described in the dependent claims and in the following description of a particular example of embodiment.

Figure 1 shows schematically a block diagram of the device with a secure module 2, which permanently stores the secret code needed to sign a document. In addition by means of said secure module said secret code allows the digital signature of predetermined electronic document or files. These documents or files are prepared by a computer 4, specifically by its central processor, and are sent to an external output device through a data cable 8 located externally and/or so that it is visible. The output device 6 allows extracting the data in a visible manner and comprises a monitor or screen or a printer or plotter. The secure module 2 is installed between the computer 4 and the output device 6, and contains exactly the same data or files as the external output device 6. The data cable 8 is suitably placed so that it is visible to the user as an extended cable, and preferably as a conventional printer or monitor cable. Because of the simple connection between the components the user can immediately see that the external output device receives the same data as the secure module, which is installed between the central processor of the computer and the external output device 6. The secure module 2 connected between them is designed specifically to check a predetermined digital signature for a predetermined electronic document.

Preferably, the secure module 2 that makes the signature comprises on one hand a processor chip card, in which is stored especially the secret code, and on the other a chip card terminal 12 to control the chip 10. The module 10 further allows, in accordance with the invention, checking whether a predetermined signature for a predetermined document is correct. In a specifically suitable manner, the computer 4 or its central unit is connected to the secure module 2 and to the external output device by a coupling component 14. This is thus a passive coupling component, preferably in the form of a T-connector, which on one side is connected to the data cable 8 connected to the

computer 4, and on the other side has its outputs 16, 18 connected to the external output device 6 or the secure module 2 through the data cables 20, 22. The coupling component 14 has no capability other than to retransmit the data that arrive from the computer 4 to both outputs 16, 18, and through the cables 20, 22 to the external output device 6 or to the chip card terminal 12. Because of the simplicity of the coupling component, which has no other function than to retransmit the data received from the computer 4 to the output device 6 and to the secure module 2, it is immediately apparent to a user that both the output device 6 and the secure module 2 have received the same data from the computer 4.

In a specific development the computer 4 is associated to a printing control 24 that replaces a conventional printer. The printing control 24 in accordance with the invention is such that when a printing instruction is issued, particularly for a postscript file, module 2 initiates the signature of the following file, which is sent to the external output device or to the printer 6 via the output 16 and the data cable 20.

List of referenced symbols

2	secure module
4	computer
6	output device
8	data cable
10	processor chip card
12	chip card terminal
14	coupling component
16, 18	output
20, 22	wire / data cable
24	printer control

CLAIMS

1. Device for producing a digital signature, comprising a processor (4) and an external output device (6), characterized in that between the processor (4),

particularly its central unit, and the external output device (6) is placed a secure module (2) which calculates the digital signature with the aid of a secret code.

2. Device according to claim 1, characterized in that the secure module (2) contains a chip card terminal (12) as well as a processor chip card (10) for permanent storage of the secret code.

3. Device according to claim 1 or 2, characterized in that connected to the processor (4) is a coupling component (4) with outputs (16, 18) that lead on one side to the external output device (6) and on the other to the secure module (2), specifically by means of data wires or cables (20, 22).

4. Device according to one of claims 1 to 3, characterized in that the output device (6) and the secure module (2) are connected to each other preferably through the coupling component (14), so that the output device (6) and the secure module (2) always receive the same data from the processor.

5. Device according to one of claims 1 to 4, characterized in that the processor (4) has a printing control designed such that when a printing instruction is issued, the signature of the data emitted by the processor (4) with the printing instruction is initiated at the secure module and specifically at the chip card terminal (12.

One sheet of drawings is accompanied.

Device for producing a digital signature

A device for producing a digital signature that comprises a processor (4) and an external output device (6). The device must be developed such that a user can be certain of signing only the desired document, and not another. It is proposed to place between the processor (4), specifically between its central unit, and the external output device (6) a secure module (2) to calculate the digital signature with the aid of a secret code.
